CMI CHR. MICHELSEN INSTITUTE

CMI BRIEF 2026:07

Digital War Participation

Contemporary wars have immediate effects beyond the physical warzone.

AUTHOR | Eva Johais

Summary

Digital technology has transformed the nature and practice of warfare. It has forced militaries to change tactics, strategies, and coordination structures, and to build up capabilities for cyberwar. More incisively, warfare has extended beyond the military remit. Digital technology enables ordinary people to participate in armed conflicts wherever they happen. This has serious implications for European states' societal peace and security.

Digital war

The current security situation has been characterised by European leaders – from the NATO Secretary General to the German Chancellor – as "We are not at war, but we are not at peace either". This description reflects that European states perceive being threatened by geopolitical rivals even if these rivals do not apply physical military force.

Russia appears to be the most imminent threat since it is waging a full-scale war in Europe. In addition, the Russian state has tried to destabilize European countries through alleged sabotage of critical infrastructure, cyberattacks, and disinformation campaigns. Similar in nature are security risks posed by China emanating from cyber-espionage, the threat of retaliation against restrictions on Chinese companies, as well as strategic dependencies on Chinese rare earth elements and production capacities and strategic vulnerabilities built-in Chinese technology.

The second Trump administration has turned the United States from a reliable NATO ally into a defector of multilateral agreements, an economic competitor ready to engage in tariff wars with the European Union, and violator of the democratic and human rights that European states hold dear.

The increasing use of non-military means to achieve political ends against adversaries has commonly come to be called 'hybrid warfare'. This combines the threat of military force with economic, informational, political, and social means to influence the domestic politics of target states.

Key Points

- Digital technology is changing military operations and ordinary people's relationship to war.
- Digital tools are increasing the reach and effectiveness of hybrid warfare.
- Labelling non-military activity 'warfare' is a political decision.
- Digital war participation has effects on the individual, societal, and international level.
- Digital war participation is eroding the distinction between civilian and combatant.
- Digital war participation requires coordinated policy responses across education, social, security and foreign policy.

Funded by the European Union

It is not a new phenomenon that non-kinetic means are used to defend national interests and security against adversaries. The Cold War remained 'cold' because the conflict parties reverted to political warfare often in the form of covert activities ranging from propaganda to sabotage, and supporting resistance movements to avoid escalation that could have caused a nuclear war.

Hybrid warfare originally referred to a military strategy that deploys special forces alongside regular forces. The concept evolved to describe an antagonistic foreign policy strategy that uses all available military and non-military means.

In the digital age, however, new tools have ramped up Cold War tactics to a new level by both increasing the effectiveness and expanding the scope of hybrid warfare. Digital technology resolves the problem that covert action used to be constrained to small-scale interferences to remain plausibly deniable. Thanks to the relative anonymity of the internet and the immediate transnational outreach through digital connectivity, it is now possible to manipulate distant individuals and infrastructures without being identified, caught, or stopped.

This digital warfare requires militaries to reorganise, restrategise, and develop know-how, tools, and infrastructure for cyberwar. Military operations change towards decentralized, information-based coordination structures of command, communications, control, and intelligence. In information wars, the strategic goal is to achieve the prerogative of interpretation instead of gaining territorial control. Cyberwar tactics employ information-based capabilities to influence, disrupt, usurp or destroy the adversary's information and communication systems. Cyberattacks include the infiltration of computer networks, denial of service (DoS) attacks, or the use of ransomware to paralyse the information-based infrastructure of military facilities, hospitals, or energy suppliers.

A practical challenge of digital warfare is that it is difficult to clearly identify perpetrators, attribute responsibility for hostile acts, and scale adequate responses. The bigger political question at stake is, however, when non-military activity passes the threshold to war. It seems reasonable to call such activity warfare if it occurs in the context of political antagonism and is employed with the intensity and purpose to be perceived by the target as a form of strategic coercion commensurable to warfare. But it is important to emphasise that declaring a war or war-like situation is a political decision serving to justify the use of force and the build-up and mobilisation of military capabilities. This is a decision that subordinates politics to military logics, diverts resources from other public sectors like education, health, or transportation, and promotes a militarisation of society.

Digital war participation

The blind spot of the 'hybrid warfare' debate is that it focuses on the antagonism between states and the impact of digital technology on foreign policy and military strategy. This perspective misses that digital technology at the same time fundamentally transforms the relationship between war and society. In contrast to previous media innovations, digital technology enables state and non-state actors alike to disseminate their perspectives on ongoing conflicts without the cooperation of traditional media gatekeepers. However, the full implications become clear if digital technologies are not merely considered as communication tools.

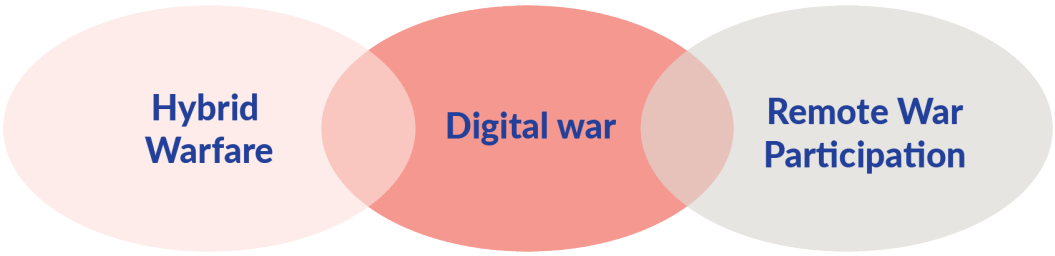
Current wars are both digitised and mediatised: the technical infrastructure of digital platforms and devices extends the possibility to participate in war to anyone, anywhere, at anytime. Digitisation thereby provides the conditions for mediatisation: digital technology does not simply transmit the perception of but actively structures the engagement with wars. Internet speed and data policies, platform design and algorithms, viral trends, popular culture and affective dispositions increasingly shape how people interact with political and military developments in warzones. The possibilities of common participation in armed conflict by digital means give rise to a new mode of participatory warfare.

Participatory warfare describes the common participation in armed conflict by digital means.

Participatory warfare spans the whole spectrum of war-related practices including propaganda, intelligence, logistics and combat. Infowarriors produce, disseminate, or verify content to produce and counter specific war narratives. Hacktivists use their skills to infiltrate the enemy's information infrastructure and volunteer data analysts process open-source data to monitor the humanitarian situation on the ground or provide useful information for military operations. Crowdfunding campaigns raise financial resources for the war efforts or donations to buy specific equipment to cover the needs of military and civilian actors. These digital activities extend the physical battlefield of current armed conflicts into global war ecologies.

For this reason, current wars do not only cause suffering and destruction in the war-affected countries but also trigger socio-political dynamics in societies far from the warzone. On the individual level, digital technology can mobilise people who would otherwise lack means or motivation to take sides in an armed conflict and justify, support, or commit acts of physical violence, criminal offences, or verbal and psychological abuse. Social media promotes empathy for distant suffering or anger about the use of brute force and smart devices make it possible to witness and act in real time. Remote war participants in the digital age are, therefore, not limited to people in the diaspora who care for friends and family and get into action during wars in their country of origin.

Figure: Contemporary warfare



In the war-affected country, remote participation may have both positive and detrimental effects: it may exacerbate and prolong the violence through moral and material support for warring parties but also help finding political solutions, foster reconciliation and build peaceful futures. Individual politicisation and possibly radicalisation can also threaten societal peace and security in remote participants' countries of residence if it leads to conflict-related polarisation and organised political action. Current wars happening elsewhere can create or reinforce divides between supporters of opposed warring parties and spark off independent conflict dynamics in the digital battlefield or in the streets. Transnational activist networks or diaspora groups may hereby become conflict actors in their own right.

With effects both at home and abroad, digital war participation evades the common division of responsibilities between state authorities – notably between the foreign ministry and the ministry of the interior. In addition, it erodes the principles of International Humanitarian Law. The contemporary ius in bello regulates the legitimate use of force during an armed conflict based on the distinction between civilians and combatant as codified in the Geneva Conventions.

Ius ad bellum defines when it is legitimate for states to apply military force. Traditionally, wars could be warranted by just reasons, right intentions, legitimate authority, and as a means of last resort. By contrast, the United Nations Charter obliges states to abstain from waging war altogether. The only exemptions from the general prohibition on the use of force are the right to self-defence against aggression and international interventions mandated by the UN Security Council.

Ius in bello concerns which acts and means are permissible during warfare.

Combatants are typically military personnel having the privilege to apply violence to enemy forces. This implies that combatants are legitimate targets of military attacks. In contrast, the participation and targeting of civilians is disincentivised. Even though it is not unlawful if civilians are harmed as a corollary of military operations, international law prohibits that civilians are deliberately made the target of attacks.

Civilians lose this protection, however, if they take actively part in hostilities. Worse still, civilian war participants do not enjoy the rights of combatants who are entitled to prisoner of war treatment and exempted from domestic persecution for acts of violence that are committed in the course of their professional activity of waging war on behalf of the state. As the Geneva Protocols did not specify the meaning of 'direct participation in hostilities', it is unclear due to which kind of actions civilians lose their immunity and when the loss of protection starts and ends.

Digital war participation is a yet-unexplored, emerging phenomenon that poses policy challenges on national and international levels and across domains from education, media, and social work, to internal security and foreign policy. It requires both further study and greater acknowledgement from policy-makers to ensure that European states are prepared for the spread of digital war participation.

Funded by the European Union

CMI CHR. MICHELSEN INSTITUTE | #WARS

Further reading

Crawford, Emily. Identifying the Enemy: Civilian Participation in Armed Conflict. Oxford: Oxford University Press, 2015.

Ford, Matthew, and Andrew Hoskins. Radical War: Data, Attention and Control in the Twenty-First Century. London: Hurst and Company, 2022.

Jonsson, Oscar, and Ilmari Käihkö, eds. Non-Military Warfare: A War of Our Time. New York: Routledge, 2026.

Kaempf, Sebastian. "The Mediatisation of War in a Transforming Global Media Landscape." Australian Journal of International Affairs 67, no. 5 (2013): 586–604.

Merrin, William. Digital War: A Critical Introduction. London, New York: Routledge, 2019.

Norman, Jethro, Matthew Ford, and Signe Marie Cold-Ravnkilde. "The Crisis in the Palm of Our Hand." International Affairs 100, no. 4 (2024): 1361–79.

Policy recommendations for European states

- **Digital competence:** States should invest in building scientific expertise about digital war participation, train school and university teachers in digital risks, support civil-society initiatives on digital conflict and mobilisation, and enhance state authorities' capacities to monitor conflict-related digital activities.
- **Social work:** Learn lessons from dealing with similar forms of politicisation, and radicalisation like far-right or Islamist extremism and apply them to digital war participation. Potentially build-up cultural and social work capacities for processing individuals' war experience, foster dialogue across political divides, and help reintegrating into civil social life.
- **Societal peace & security:** State authorities, security forces and educational institutions should anticipate conflict-related politicisation, radicalisation, and polarisation and be prepared to address illegal and violent activities.
- **Review legislation:** Digital war participation challenges the civil-military distinction on which International Humanitarian Law is based. It is particularly important to clarify the concept of direct participation in hostilities to be able to identify participants that can practically and legitimately become the targets of defensive measures.
- **International conflict management:** Consider the role of transnational activist networks and diaspora groups in conflict analysis. Involve them as stakeholders or mediators in conflict resolution and peacebuilding initiatives.
- **Cross-departmental collaboration:** Digital war participation affects several policy areas including digitization, education, foreign affairs, internal security, and justice. Government departments should establish cross-departmental working groups to ensure state-of-art knowledge about the emergent phenomenon and coordinate appropriate strategies.

This policy brief is part of the ERC-funded **Hashtag Wars Project**.

CMI (Chr. Michelsen Institute)
Phone: +47 47 93 80 00
Phone from abroad: +47 55 70 55 65
E-mail: cmi@cmi.no

P.O. Box 6033,
N-5892 Bergen, Norway
Visiting address:
Jekteviksbakken 31, Bergen

ISSN 0809-6732 (print)
ISSN 0809-6740 (PDF)